توصیه های امنیتی برای استفاده از شبکه و اینترنت

انتخاب و محافظت از کلمات عبور

کلمات عبور بخش مهمی از امنیت کامپیوتر هستند و در حقیقت در خط مقدم حفاظت از اکانت کاربران قرار می گیرند. یک کلمه عبور نامناسب ممکن است منجر به سوءاستفاده از کل شبکه شود. بهمین دلیل تمام کارمندان که به اینترنت دسترسی دارند مسوول انتخاب کلمه عبور مناسب و محافظت از آن هستند.

سیاست کلی

- ✓ تمام کلمات عبور در سطح سیستم باید حداقل سه ماه یکبار عوض شوند.
- ✓ تمام کلمات عبور سطح کاربر (مانند ایمیل یا کامپیوتر) باید هر شش ماه تغییر کنند که البته تغییر چهار ماهه توصیه می شود.
- ✓ اکانتهای کاربری که مجوزهای سطح سیستم دارند باید کلمات عبوری داشته باشند که با کلمات عبور دیگر اکانتهای آن کاربر متفاوت باشد.
- ✓ کلمات عبور نباید در ایمیلها یا سایر شکلهای ارتباطات الکترونیکی درج شوند.
- ✓ باید رهنمونهای زیر در تمام کلمات عبور سطح سیستم و سطح کاربر رعایت شود.

کلمات عبور ضعیف معمولا مشخصات زیر را دارند:

- ✓ کلمه عبور شامل کمتر از هشت حرف است.
- ✓ کلمه عبور کلمه ای است که در یک فرهنگ لغت یافت می شود.
- ✓ کلمه عبور کلمه ای است که کاربرد عمومی دارد مانند:
  - نام خانوادگی، حیوانات اهلی، دوستان، همکاران، شخصیت های خیالی و غیره
  - نامها و اصطلاحات کامپیوتری، فرمانها، سایتها، شرکتها، سخت افزار و نرم افزار.
  - نام شرکت یا کلمات مشتق شده از این نام.
  - تاریخ های تولد و سایر اطلاعات شخصی مانند آدرس ها و شماره های تلفن.
  - الگوهای کلمات یا شماره ها مانند aaabbb، qwerty، zyxwvuts، ۱۲۳۳۲۱ و غیره.
  - هرکدام از عبارات فوق بطور برعکس.
  - هرکدام از عبارات فوق که تنها با یک رقم شروع یا به آن ختم می شود.

کلمات عبور مناسب مشخصات زیر را دارند:

- ✓ شامل هم حروف کوچک و هم بزرگ هستند (a-z و A-Z)
- ✓ علاوه بر حروف از ارقام و نشانه ها هم در آنها استفاده می شود مانند ۹-۰ و !@#$%^&*()_+|~='{}[];<>?./
- ✓ حداقل هشت حرف دارند.
- ✓ کلمه ای در هیچ زبان، گویش یا صنف خاص نیستند.
- ✓ برپایه اطلاعات شخصی، اسم یا فامیل نیستند.
- ✓ کلمات عبور هرگز نباید نوشته یا جایی ذخیره شوند. سعی کنید کلمات عبوری انتخاب کنید که بتوانید براحتی در ذهن داشته باشید. یک روش انجام این کار، ایجاد کلمه عبور بر پایه یک ترانه یا عبارت

است. برای مثال عبارت "This May Be One Way To Remember" و کلمه عبور می تواند "TmB۱w۲R!" یا "Tmb۱W>r~" یا انواع دیگری از همین الگو باشد.

توجه: این مثالها را بعنوان کلمه عبور استفاده نکنید.

استانداردهای حفاظت از کلمه عبور

از کلمات عبور مشترک برای اکانتهای دانشگاه و دسترسی های شخصی استفاده نکنید. تا جایی ممکن است، از کلمه عبور مشترک برای نیازهای مختلف دانشگاه استفاده نکنید. برای مثال، برای سیستمهای مهندسی یک کلمه عبور انتخاب کنید و یک کلمه عبور دیگر برای سیستمهای IT .کلمات عبور دانشگاه با هیچ کس از جمله همکاران در میان نگذارید. باید با تمام کلمات عبور بصورت اطلاعات حساس و محرمانه برخورد شوند.

مراقب ایمیل ها و پیام های جعلی باشید.

مراقب پیامهایی که ارسال کننده از عناوینی چون مدیر، مدیران یا بخش پشتیبانی ۱۰۰۰استاد استفاده کرده است باشید. حتی اگر این پیام از سمت ایمیل های سایت مانند info@۱۰۰۰ostad.com آمده باشد. چرا که شیوه هایی برای ارسال ایمیل های جعلی اینچنینی وجود دارد.

دیده شده است در مواردی افرادی با سوء استفاده از عنوان مدیر سایت و با ارسال ایمیل یا درج نظر از کاربران خواسته اند برای مواردی مثل عدم حذف یا افزایش امکانات، کلمه عبور خود را برای آنها ارسال کنند یا در صفحه دیگری وارد کنند. قطعا مدیریت ۱۰۰۰استاد نیازی به دانستن کلمه عبور شما یا دریافت مجدد آن ندارد بنابراین هر گونه درخواست اینچنینی جعلی و در جهت فریب کاربران می باشد.

ایمیل و کلمه عبور خود را فقط در صفحه اول یا در بخش ورود کاربران سایت وارد کنید.

کلمه عبور خود را فقط در آدرس اصلی سایت یا در بخش ورود کاربران سایت وارد کنید. سعی کنید هر باری که می خواهید کلمه عبور خود را وارد کنید، در نوار آدرس مرورگر خود، آدرس سایت را چک کنید. ورود کلمه عبور شما در هر صفحه یا آدرس دیگری به غیر از آدرس اصلی سایت به احتمال بسیار زیاد به معنی لو رفتن و هک شما خواهد بود. یکی از شیوه های رایج برای فریب و هک کاربران و گرفتن کلمه عبور آنها، طراحی صفحات بسیار شبیه به سایتهای مهم مثل سرویسهای ایمیل است. بنابراین با دقت به آدرس صفحه (در نوار آدرس مرورگر) و ورود کلمه عبور در سایت اصلی جلوی سوء استفاده های احتمالی را بگیرید.

مراقب ایمیلهای خود باشید.

ایمیل خصوصی که در هنگام ثبت نام از شما پرسیده میشد، برای ارسال کلمه عبور، در زمانی که آنرا فراموش کرده باشید استفاده می شود و در سایت نیز نمایش داده نمیشود. پس آن را صحیح و با دقت وارد کنید و همچنین توصیه می کنیم که از این ایمیل در مسنجرها (مانند یاهو مسنجر) استفاده نکنید زیرا احتمال هک شدن آی دی و ایمیل هایی که در مسنجرها استفاده میشود بیشتر است و بسیاری از مشکلات امنیتی سایتها (در تمامی سرویس دهندگان) نیز به همین دلیل است. توجه داشته باشید که هک ایمیل شما می تواند باعث سوء استفاده های دیگر و به خطر افتادن امنیت مطالب شما شود. در صورتیکه به هر دلیلی مشکلی برای ایمیل شما ایجاد شد سریعا در بخش تنظیمات خود، آدرس ایمیل خصوصی و همچنین کلمه عبور خود را تغییر دهید.

موارد امنیتی را هنگام استفاده از کامپیوتر در نظر بگیرید.

- ✓ از دانلود برنامه ها و فایل های غیر مطمئن و بخصوص فایلهای اجرایی(مثل فایلهای EXE)از سایتهای غیر معتبر پرهیز کنید و از کامپیوتر خود با نصب آخرین نسخه های نرم افزاری آنتی ویروس و همچنین به روز رسانی سیستم عامل و مرورگر اینترنت محافظت کنید.
- ✓ توجه داشته باشید که برنامه های کوچکی وجود دارند که در صورت دانلود و اجرا توسط کاربر، اطلاعات مختلف موجود در کامپیوتر و از جمله کلمات عبور مختلف وی را در اختیار هکرها قرار می دهد. بنابراین از دانلود فایلهای اجرایی به هر عنوان (مثل بازی کامپیوتری، موسیقی، نرم افزار مفید و ...) از سایتهای غیر معتبر خودداری کنید.
- ✓ در صورتی که در کافی نت، دانشگاه و یا دیگر مراکز عمومی از سایت استفاده میکنید، مطمئن شوید که کامپیوتر فوق از نظر تروجان یا برنامه های جاسوسی پاک است و ترجیحا در این شرایط کلمه عبور خود را بصورت مرتب تغییر دهید.
- ✓ در سایتهای شخصی یا در هنگام chat اطلاعاتی مانند آدرس خود یا شماره تلفن خود را در اختیار دیگران قرار ندهید.
- ✓ اگر chat می کنید یا با شخصی بوسیله e-mail ارتباط دارید و به او اطمینان کامل ندارید منطقه مورد سکونت خود را به او اطلاع ندهید.
- ✓ اطلاعات شخصی از قبیل آدرس یا شماره حساب بانکی یا شماره کارت اعتباری را در email ها وارد نکنید یا آنها را در فیلدهای خواسته شده در یک سایت غیر ایمن وارد نکنید بنابراین همیشه قبل از دادن این اطلاعات مطمئن شوید در یک سایت ایمن هستید و بعد شماره کارت اعتباری خود را برای خرید وارد کنید. تشخیص یک سایت ایمن از غیر ایمن معمولاً بسیار ساده است زیرا یک سرور ایمن با "https://" در فیلد

آدرس ظاهر می شود و حال آنکه یک سرور غیر ایمن با "http//:" شروع می شود سرورهای ایمن اطلاعات شما را به رمز در می آورند.بنابراین هیچکس به غیر از شما و کامپیوتری که در سمت دیگر است نمی تواند این اطلاعات را در یافت کند.

- ✓ از یک ویروس یاب استفاده کنید. از سایتهای غیر مطمئن یا email های مشکوک فایلی Download نکنید. حتی اگر یک ویروس یاب دارید خیلی مواظب باشید زیرا ممکن است با ویروس جدیدی مواجه شوید که نرم افزار ضد ویروس شما نتواند آن را تشخیص دهد برای یک حفاظت خوب همیشه آنتی‌ویروس خود را date to up (به روز) نگه دارید.

هشدار در باره نامه ها و پیامهای وسوسه کننده

بانک‌ها و موسسات اعتباری هیچ‌گاه از طریق نامه‌های الکترونیکی اطلاعات محرمانه شما را درخواست نمی‌کنند. بنابراین هرگاه در صندوق پستی خود نامه‌هایی از این دست را مشاهده کردید به سرعت آن را حذف کنید. همچنین کلاهبرداران اینترنتی ممکن است به شیوه‌های مختلف درصدد جلب اعتماد شما برآیند، بنابراین از ارایه اطلاعات حساب بانکی یا مشخصات خود با آنان خودداری کنید.

مطمئن باشید که کلاهبرداران اینترنتی با مراجعه به سایت‌های مختلف می‌توانند اطلاعات شخصی افراد را به دست آورند. بنابراین در صورت مشاهده مشخصات خود به طور کامل و دقیق در نامه آن‌ها، سعی کنید حساب بانکی خود را تغییر دهید.

در صورت وارد شدن به بازی این کلاهبرداران، سعی کنید پیش از واریز کردن هرگونه وجهی به حساب آن‌ها، مراتب را از طریق وزارت امور خارجه و سفارتخانه‌های مربوط به کشور فرستنده نامه پیگیری کنید.

با توجه به اینکه بیشتر کلاهبرداران درخواست واریز پول به حساب‌های خارجی را دارند، بنابراین اگر کاربر مبالغ هر مرحله را به بانک خارجی اعلام شده پرداخت کند، در مراحل بعدی نیز هزینه‌های بالاتری از او درخواست می‌شود. این فرآیند تا جایی پیش می‌رود که مبالغ زیادی از کاربر قربانی اخاذی می‌شود. این در حالی است که پس از پیگیری مالباخته برای روشن شدن وضعیت خود، کلاهبرداران به بهانه‌های مختلف طفره می‌روند یا ارتباط ایمیلی خود را قطع می‌کنند.

بنابراین به تمامی کاربران هشدار داده می‌شود اگر نامه‌های الکترونیکی با عنوان برنده شدن جایزه، استخدام و... را دریافت کردید که در متن آن نامه‌ها، به هر طریقی هزینه‌هایی را درخواست کرده‌اند، هویت فرستنده را از طریق نمایندگی‌های معتبر خارجی بررسی کنید تا در دام کلاهبرداران اینترنتی گرفتار نشوید.

این قبیل کاربران متخلف حس طمع کاربران قربانی را تحریک می‌کنند و پس از تطمیع آنان، اهداف شوم خود را به مرحله اجرا می‌گذارند. بخش دیگری از کلاهبرداری‌ها نیز از طریق تماس با منازل، شرکت یا تلفن‌های همراه انجام می‌شود؛ به گونه‌ای که پس از تماس با شماره‌ای که به صورت تصادفی انتخاب شده است، اعلام می‌کنند که شما در قرعه‌کشی خاصی یک دستگاه ساعت یا ماشین حساب برنده شده‌اید.

در اینجا نیز با تطمیع افراد، نشانی محل سکونت آن‌ها را دریافت می‌کنند و پس از مراجعه به محل دریافتی، هدیه‌ای باارزش پایین را تحویل می‌دهند. در کنار آن نیز یک کارت اینترنتی با مدت کارکرد زیاد و با قیمت ارزان‌تر از کارت‌های موجود در بازار را به قربانی می‌فروشند که در بیشتر موارد، بی‌اعتبار است.

در مورد تلفن همراه نیز پیامی کوتاه از یک شماره نامشخص ارسال و اعلام می‌شود که شما برنده شارژ رایگان شده‌اید و با ارسال کد مندرج در پیام کوتاه به شما هزینه مکالمه رایگان هدیه داده می‌شود. این در حالی است که کد مذکور باعث کم شدن مقدار هزینه مکالمه موجود در حساب قربانی می‌شود و آن مقدار هزینه را به فرستنده پیام کوتاه انتقال می‌دهد. در این خصوص نیز هشدار داده می‌شود اگر کسی با شماره تلفن شهروندی تماس گرفت، ممکن است قصد اخاذی یا کلاهبرداری داشته باشد یا حداقل مشخصات هویتی و سکونت مخاطب را به دست بیاورد و در آن صورت مشکلاتی را برای شهروندان ایجاد خواهد کرد. بنابراین شهروندان برای پیشگیری از بروز مشکلات مالی و امنیتی،

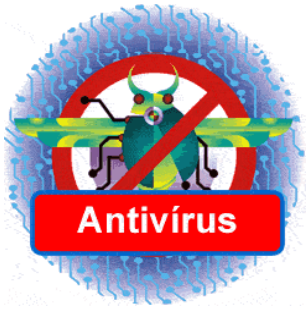
لازم است پیش از هر پاسخی به مخاطبان تلفنی یا اینترنتی ابتدا از هویت واقعی آنان اطمینان حاصل کنند و پس از آن پاسخ دهند.

نسخه پشتیبان از اطلاعات مهم تهیه کنید

از همه اطلاعات خود نسخه پشتیبان یا بک آپ تهیه کنید. یک کرم یا تروجان نفوذی برای از بین بردن همه اطلاعات شما کافی است .انتخاب کلمه عبور مناسب را سرسری نگیرید :کلمات عبوری انتخاب کنید که معقول و منطقی بوده و حدس زدن آنها دشوار باشد. همیشه کلمات عبور پیش فرض را تغییر دهید.

استفاده از نرم افزارهای محافظتی (مانند ضدویروس ها) و به روز نگه داشتن آنها

از وجود ضدویروس بر روی دستگاه خود اطمینان حاصل کنید. این نرم افزارها برای محافظت از کامپیوتر در برابر ویروس های شناخته شده به کارمی روند و در صورت استفاده از آنها کاربر نیاز به نگرانی در مورد ویروس ها نخواهد داشت. در شرایطی که روزانه ویروس های جدید تولید شده و توزیع می شوند، نرم افزارهای ضدویروس برای تشخیص و از بین بردن آنها باید به صورت منظم به روز شوند. برای این کار می توان به سایت شرکت تولید کننده ضدویروس مراجعه کرد و اطلاعات لازم در مورد نحوه به روز رسانی و نیز فایل های جدید را دریافت نمود. عموما نرم افزارهای ضدویروس ابزار های به روز رسانی و زمان بندی این فرایند را در خود دارند. برای مطالعه بیشتر در مورد ویروس ها و آشنایی با طرز کار و قابلیت های ضدویروس ها .



سیستم عامل رایانه را به روز نگه دارید

سیستم عامل خود را به طور مرتب به روز کرده و تمامی وصله های امنیتی عرضه شده توسط شرکت طراح هر سیستم عامل را بارگذاری و نصب کنید.

مراقب نرم افزارهای ضعیف امنیتی باشید

حتی الامکان از استفاده از نرم افزارهای ضعیف و در معرض حمله خودداری کرده و قابلیت های خودکار نامطمئن آنها به خصوص در نرم افزارهای ایمیل را از کار بیندازید.

- ✓ رمزگذاری اطلاعات:

از نرم افزارهای رمزگذاری اطلاعات مانند PGP در زمان ارسال ایمیل استفاده کنید. از این نرم افزار می توانید برای حفاظت از کل هارددیسک خود نیز استفاده کنید.

- ✓ نصب نرم افزارهای شناسایی عوامل نفوذی را فراموش نکنید:

حتماً نرم افزاری برای شناسایی نرم افزارهای مخرب جاسوس روی رایانه تان نصب کنید. حتی بهتر است چندین نرم افزار برای این کار نصب کنید. برنامه های سازگار با دیگر نرم افزارهای مشابه مانند SpyCop انتخاب های ایده آلی هستند.

حفاظ شخصی ZoneAlarm

استفاده از حفاظهای شخصی، در دنیای کنونی که اغلب حملات امنیتی و ویروس‌ها، کاربران عادی خانگی را هدف قرار داده‌اند، اهمیتی ویژه یافته است.

مهم‌ترین امکانات و قابلیت‌های این نرم‌افزار را می‌توان به‌صورت زیر برشمرد :

- ✓ محدود ساختن دسترسی نرم‌افزارهای مختلف بر روی رایانه

این نرم‌افزار قابلیت بررسی وضعیت ارتباط نرم‌افزارهای نصب شده بر روی سیستم با شبکه را داراست. لذا در صورتی‌که نرم‌افزاری ناشناس سعی در تماس به شبکه داشته باشد، می‌توان این دسترسی را محدود ساخت.

- ✓ محدودیت بر روی آدرس‌ها، پورت‌ها و پروتکل‌ها

توسط این امکان می‌توان از دسترسی‌هایی که از بیرون از رایانه‌مان صورت می‌گیرد، در قالب آدرس IP، پورت و پروتکل مورد نظر آگاهی یافت و در صورت نیاز این دسترسی را بست. از سوی دیگر می‌توان آدرس‌ها، پورت‌ها و پروتکل‌هایی که دسترسی از طریق آن‌ها به سیستم مانعی ندارد را مشخص نمود.

- ✓ امکان حفاظت از اطلاعات شخصی

توسط این امکان، و با پاک کردن Cacheهای مختلف پرونده‌ها، آدرس‌ها، Cookieها و دیگر اطلاعات شخصی حساس مشابه، می‌توان از درز کردن اطلاعات شخصی مهمی از این قبیل به شبکه جلوگیری نمود.

- ✓ سیستم محافظت از سرویس پست الکترونیک

توسط این امکان، نامه‌های ورودی به سیستم، که احتمال آلوده‌گی آن‌ها وجود دارد را مسدود ساخت. از سوی دیگر در صورت آلوده بودن سیستم به ویروس‌هایی که خود را از طریق ارسال نامه به دریافت‌کننده‌گانی که آدرس آنها در فهرست آدرس برنامه‌ی ارسال پست‌الکترونیک موجود است، منتشر می‌کنند، می‌توان جلو این انتشار را با مسدود ساختن نامه‌های ارسالی گرفت.

- ✓ صدور اخطارهای امنیتی

جدا از گزارش حملات احتمالی، درصورتی‌که قصد ارسال اطلاعات به شبکه را داشته باشیم، هشدارهای امنیتی از سوی این نرم‌افزار توجه استفاده کننده را به دقت بیشتر در این زمینه جلب می‌کند.

- ✓ تغییر سطح امنیت به صورت خودکار

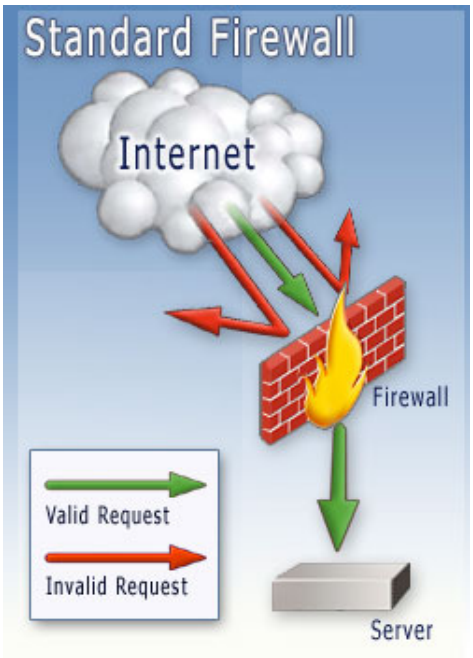
در صورت بروز حملات متعدد امنیتی، نرم‌افزار به طور خودکار سطح حفاظت را بالاتر می‌برد. این امکان احتمال دفع حملات را بالا می‌برد.

آخرین نگارش این نرم‌افزار نسخه‌ی ۴ است که کماکان بیشترین اقبال را در میان این دسته از نرم‌افزارها به خود جلب کرده، و بیشترین محبوبیت و کارایی را در میان کاربران عادی یافته است.

محافظت از کامپیوتر در برابر نفوذ با استفاده از حفاظ(Firewall)

حفاظ دیواری مجازی بین سیستم کامپیوتری و دنیای بیرون ایجاد می کند. این محصول به دو صورت نرم افزاری و سخت افزاری تولید می شود و برای حفاظت کامپیوترهای شخصی و نیز شبکه ها به کار می رود. حفاظ داده های غیر مجاز و یا داده هایی که به صورت بالقوه خطرناک می باشند را فیلتر کرده و سایر اطلاعات را عبور می دهد. علاوه بر این حفاظ در شرایطی که کامپیوتر به اینترنت وصل است، مانع دسترسی افراد غیرمجاز به کامپیوتر می شود.

از دیوار آتش یا firewall شخصی استفاده کنید. پیکربندی فایروال خود را به دقت انجام دهید تا از نفوذ به رایانه شما جلوگیری شود. این فایروال ها همچنین مانع وارد آمدن خسارت به شبکه ها و سایت هایی که به آنها متصل هستید، شده و قادر به تشخیص ماهیت برنامه هایی هستند که تلاش می کنند به شبکه اینترنت متصل شوند.



حذف برنامه های دسترسی از راه دور

امکانات روی رایانه که به آنها احتیاج ندارید را از کار بیندازید.به خصوص برنامه های کاربردی که دسترسی به رایانه شما را از راه دور ممکن می کنند مانندRemote Desktop ، RealVNC و NetBIOS را حذف یا به اصطلاح disable کنید.

از امنیت شبکه های رایانه ای اطمینان حاصل کنید

در جهت ایمن سازی شبکه های رایانه ای و به خصوص شبکه های بی سیم بکوشید. شبکه های وای – فای(بیسیم) خانگی را با کلمه عبوری با حداقل ۲۰ کاراکتر ایمن کنید. پیکربندی اتصال لپ تاپ خود به شبکه را به گونه ای انجام دهید که برقراری ارتباط تنها در حالت Infrastructure اتفاق بیفتد.

هکرها روز به روز به روش های پیچیده تری برای سرقت اطلاعات کاربران روی می آورند ولی شما با رعایت همین نکات ساده، آسیب پذیری سیستم های رایانه ای خود را به حداقل خواهید رساند.

خودداری از به اشتراک گذاشتن منابع کامپیوتر با افراد غریبه

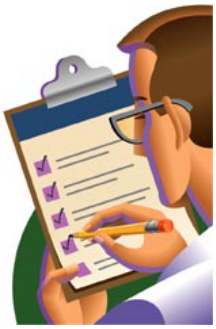
سیستم های عامل این امکان را برای کاربران خود فراهم می آورند که با هدف به اشتراک گذاری فایل، دسترسی دیگران را از طریق شبکه و یا اینترنت به دیسک سخت محلی فراهم آورند. این قابلیت امکان انتقال ویروس از طریق شبکه را فراهم می آورد. از سوی دیگر در صورتی که کاربر دقت کافی را در به اشتراک گذاشتن فایل ها به عمل نیاورد، امکان مشاهده فایل های خود را به دیگرانی که مجاز نیستند ایجاد می کند. بنابراین درصورتی که نیاز واقعی به این قابلیت ندارید، به اشتراک گذاری فایل را متوقف نمایید.

قطع اتصال به اینترنت در مواقع عدم استفاده

به خاطر داشته باشید که بزرگ راه دیجیتال یک مسیر دوطرفه است و اطلاعات ارسال و دریافت می شوند. قطع اتصال کامپیوتر به اینترنت در شرایطی که نیازی به آن نیست احتمال اینکه کسی به دستگاه شما دسترسی داشته باشد را از بین می برد.

بررسی منظم امنیت کامپیوتر

در بازه های زمانی مشخص وضعیت امنیتی سیستم کامپیوتری خود را مورد ارزیابی قرار دهید. انجام این کار در هر سال حداقل دو بار توصیه می شود. بررسی پیکربندی امنیتی نرم افزارهای مختلف شامل مرورگرها و حصول اطمینان از مناسب بودن تنظیمات سطوح امنیتی در این فرایند انجام می شوند.



حصول اطمینان از آگاهی اعضای خانواده و یا کارمندان از نحوه برخورد با کامپیوترهای آلوده

هر کسی که از کامپیوتر استفاده می کند باید اطلاعات کافی در مورد امنیت داشته باشد. چگونگی استفاده از ضدویروس ها و به روز رسانی آنها، روش گرفتن وصله های امنیتی و نصب آنها و چگونگی انتخاب گذرواژه مناسب از جمله موارد ضروری می باشد.